

FIG. 1 (PRIOR ART)

	204		206	208 2	210 21	2 2	212 214 216 218	9	18	220 22	222	224
OPERATION		CYCLE	-	į	B	q	ţ	_	temp	MEMORY READ (FIRST CYCLE) (MR1)	MEMORY READ (SECOND CYCLE) (MR2)	MEMORY WRITE (MW)
a = S[i+1]		0								lils		
		-	+								lils	
j=j+a		2		j + MR2	MR2					,		
[]S = q		e e								[lls		
		4									Siji	
, t = g	S[i] = b, t = a + b, temp = plain[i]	2				MR2	MR2 + a			[]]blain		S[i] = MR2
S[]]=a		9								Sti	[j]ujaj	S[j] = a
		7 (0)							MR2		Sltj	
lox o	temp = temp XOR S[t]	8 (1)							temp XOR MR2			
±		9 (2)						+				cipher[I] = temp
l	l		l			l		l				

FIG. 2 (PRIOR ART)

700

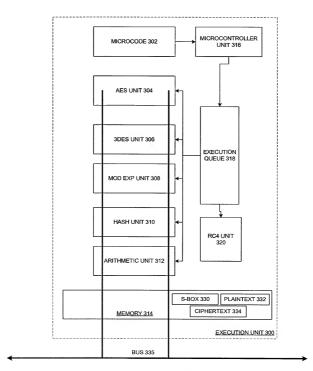


FIG. 3

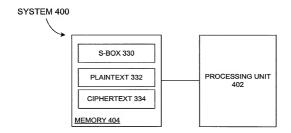
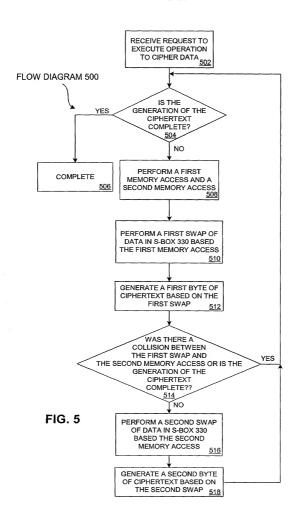
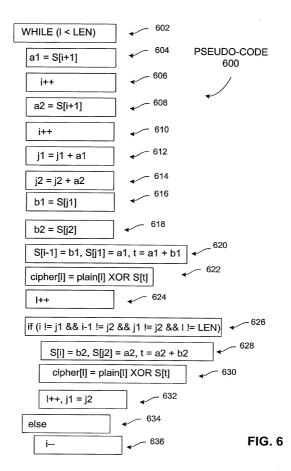


FIG. 4

005655.P007
"Speculative Execution for Data Ciphering Operations"
David A. Carlson





MEM. MEM. READ READ (1ST (ST) (MEM. (1ST)	01 02 t temp1 temp2 (MR1) (MR2)	iis	ils .	ES SIL	SU11 SI	WR2     +1	MR2 MR2 S[[2] plain[]] S[1-1] = MR2 + a1		MR2 S(t) S(2) S(2) = a2	MR2   MR2   1+1   Plain[i] S[t] S[t] = MR2	temp1 XOR plain[j]	MR2 S[t]   cipher[I-1] = temp1	bis .	temp2 XOR MD2	7,11,7				cipher[I] = temp2				
2	ē .			MR2		J2 + MR2 MF									L	-					_	-	$\parallel$
Σ		-	+	j1+ MR2		πΣ	-			27		Н			H	H	$\vdash$	H	-				+
-	- 1	+	1	Ξ											İ	ľ		T			-	-1	-
70,0	3	0	-	2	3	4	ıo		9	7	8 (0)	9 (1)	10 (2)	11(3)	12 (4)	13 (5)	14 (6)	15 (7)	16 (8)			9	
Cityana		+ a1 = S[i+1], i+		4 a2 = S[[+1], [++, j1 = j1 + a1		++, S[11]=a1,  2=j2+a2	b2 = S[j2], t= a1 + b1 S[i-1] = b1	if(i != j1 && i-1 != j2 && ▼ j1 != j2 && ! != len)	◆ S[[2] = a2	t=a2+b2, S[i]=b2,			·-							else	-	:	<u>:</u>

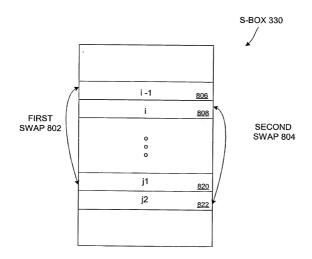


FIG. 8

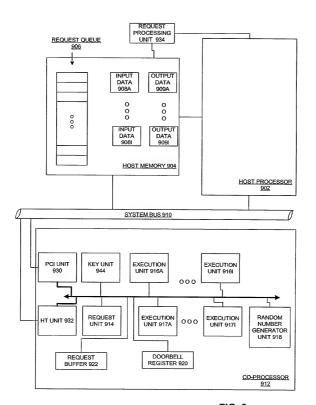


FIG. 9